Taking a Risk-Based Approach to Maritime Domain Awareness

Maritime Domain Awareness is an essential enabler of maritime security, but we must pursue it based upon a deliberate and risk-based approach.

by MR. F. R. (JOE) CALL III
Strategic Advisor to the U.S. Coast Guard Assistant Commandant for Intelligence and Criminal Investigations.

MARITIME DOMAIN AWARENESS IS THE EFFECTIVE UNDERSTANDING OF ANYTHING ASSOCIATED WITH THE MARITIME DOMAIN THAT COULD IMPACT THE SECURITY, SAFETY, ECONOMY, OR ENVIRONMENT OF THE UNITED STATES.

As a member of the early team working on the Martine Domain Awareness (MDA) concept, my fellow team members and I struggled to come up with an acceptable definition for "Maritime Domain Awareness." I witnessed the initial demands for complete understanding of the maritime domain and the dawning recognition that this was unrealistic and unachievable. One phrase, "effective understanding" remained fairly consistent throughout our deliberations. We felt that this phrase accurately conveyed the amount of information necessary for understanding and responding to potential threats to U.S. interests in the maritime domain.

Once defined, it remained for the U.S. Coast Guard and its federal and global maritime partners to achieve this level of understanding of the maritime domain. The concept of Maritime Domain Awareness encompasses a variety of maritime missions and threats. Under the classification of maritime security, MDA includes, for example, counterterrorism, counternarcotics, alien migration interdiction operations, and protection of living marine resources. Additionally, MDA embraces the notion of promoting maritime commerce and not impeding it. In furtherance of these far-ranging goals, Maritime Domain Awareness calls for an expansive maritime command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) effort that collects, fuses, analyzes, and shares information and intelligence on an unprecedented level.

It is a holistic C4ISR architecture that transcends conventional thinking and includes varied sources and methods. The types of information that will make MDA effective include a combination of situational awareness, current intelligence, and predictive intelligence. The effort necessary for Maritime Domain

Awareness spans a continuum from a human lookout or closed-circuit television in a port facility to highly classified systems euphemistically called "national technical means." It encompasses open-source reporting, proprietary commercial data, or clandestine human intelligence sources. In the quest for MDA, all-source must truly mean all-source.

Prudent Maritime Domain Awareness

Acknowledging the "effective" requirement of MDA means there must be careful analysis of maritime threats versus vulnerabilities to justify the ambitious objectives of achieving Maritime Domain Awareness. For example, if the most likely maritime threat is a vessel-borne improvised explosive device (Figure 1), that type of threat requires a different type of awareness than that which open ocean surveillance and long-range tracking capabilities provide. In this threat scenario, information and intelligence on adversaries' intentions and capabilities become the requirement.

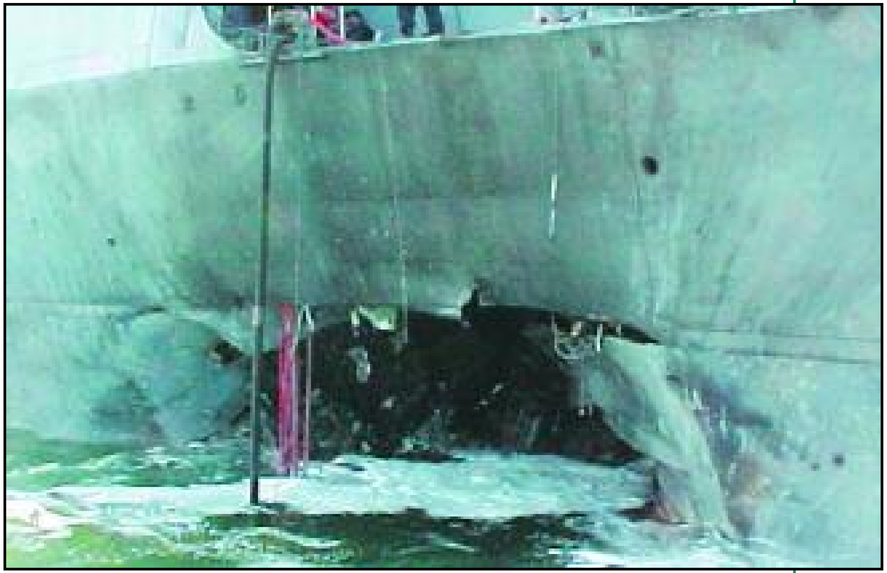

Figure 1: The attack on the *USS Cole*, from a vessel-borne improvised explosive device, represents one of the most likely maritime threat scenarios. Photo courtesy of the U.S. Department of Defense.

Unfortunately, in an uncertain world where risk management is necessary, all too often the concepts of threat and vulnerability are confused, sometimes used interchangeably and incorrectly. Such imprecise use of terms can hinder the decision of where next to invest our limited resources. Where vulnerabilities rather than threats receive too much weight, it is easy to rapidly expend resources we can ill afford. The effort to enhance MDA must judiciously examine threats and vulnerabilities before determining and responding to risk.

Without some insight into adversaries' intentions, capabilities, and target criticality we cannot effectively identify potential risks that result from credible threat reporting or highly critical targets. Ultimately, risk must drive our Maritime Domain Awareness investment strategy. Still, risk analysis is a difficult balancing act among threats, vulnerability, and criticality. All these factors must be considered. In determining threat, intelligence is the key component. There can be no substitute. Vulnerabilities often seem boundless and daunting. Criticality, on the other hand, is based on many factors that can be assessed, such as the economic value and historical and cultural significance of the potential target.

MDA Focus

There is no denying that MDA is a key enabler of maritime security, and achieving maritime security is directly tied to countering potential threats and addressing risks. As large as the global maritime domain is, a conscious and deliberate assessment of threats, vulnerabilities, criticality, and ultimately, how they translate into risks, will help narrow the view or information necessary to have the effective understanding needed for performing maritime missions. This assessment will point to the need to focus our MDA attention on specific geographic regions, functions, and activities. For example, the maritime threat of illicit drugs and illegal migration remain predominately a Caribbean, Latin American, or Eastern Pacific concern. Fisheries concerns have a limited geographic focus. Shipping risk (Figure 2) is not universal or equal in all segments of maritime commerce.

It is not perfect, but analyzing threat and risk means that Maritime Domain Awareness can vary geographically and functionally and still be effective. In some cases, general awareness is effective, in other instances, such as in a strategic port or a high-consequence vulnerability, detailed awareness is a prerequisite to be effective.

Coordination of Intelligence

This is where intelligence plays a vital role. Intelligence fusion and analysis is the value-add to the massive amounts of information collected for enhancing MDA. This requirement was recognized in the "National Strategy for Maritime Security" and its eight supporting plans. It was further developed by the call for close coordination and alignment of the "National Plan to Achieve Maritime Domain Awareness," and the "Global Maritime Intelligence Integration Plan" (GMII). At its essence the GMII plan calls for "leveraging legacy intelligence capabilities, existing policy and operational relationships to

Figure 2: Container ships pose a vulnerability that does not necessarily translate into a threat. USCG Photo by PA3 Stacey Pardini.

integrate all available data, information and intelligence."[1] The overarching requirement will be to "identify, locate, and track potential threats to the United States maritime interests."[2] In this way, the GMII effort serves the goal of enhancing MDA through current and predictive intelligence while also directly supporting maritime security planning and operations.

Many have asked for distinctions between intelligence and MDA, between situational awareness and intelligence. I offer that they are integral to each other and exist along a continuum. You cannot separate them without diminishing the whole. The capabilities and activities that are inherently intelligence related are also the capabilities and activities that help create situational awareness. Therefore, with a foundation based on the GMII plan, we can improve our ability to determine and track maritime threats, create situational awareness, share information, and make genuine progress in achieving Maritime Domain Awareness.

Managing Maritime Domain Awareness

To summarize, the goal of complete understanding of the maritime domain is as laudable as it is unrealistic. Therefore, the United States along with its allies and global partners in maritime security must invest intelligently, based not on an exhaustive set of vulnerabilities we cannot afford to address, but rather on threats and risks we can validate. We must accept and adapt to MDA limits. We must triage our requirements and manage our expectations. There are insufficient resources and little mandate for the complete transparency into maritime activity that seems so pervasive in some circles.

It is a legitimate question and a mark of good stewardship to ask if we have seen the level of maritime threats (not vulnerabilities) to justify huge expenditures on maritime C4ISR initiatives directed at global Maritime Domain Awareness, rather than specific maritime threats. Assessments have concluded the best approach may not be collecting more data, but improving the fusion and analysis of existing data sources to better determine threat. In this area, automated anomaly detection and decision tools may be valuable, but they cannot be a substitute for the hard work of intelligence analysis conducted by trained maritime intelligence analysts.

As we implement a Maritime Domain Awareness strategy, we may need to direct our attention and resources on more focused and achievable objectives that address identified threats or the highest risks. Technology holds promise, but we are far from a world of sensors and information transparency that can completely answer the challenge of global Maritime Domain Awareness. The best way we may achieve that progress may be represented as a spiral, moving toward improved open-ocean surveillance, while advancing in other collection, fusion, and analysis areas that allow insights into our adversaries' capabilities and intentions. To achieve appropriate levels of Maritime Domain Awareness, we must enter into rigorous analysis and debate that accurately validates the maritime threat, reviews MDA requirements, determines the highest vulnerabilities, and proposes risk-based solutions that will not break the budget.

About the author: *Mr. Joe Call is a retired U.S. Coast Guard commander. He has extensive experience and expertise in intelligence, maritime security, and national security issues and has served in a variety of high-level assignments including the White House Military Office and on the National Security Council staff.*

Endnotes

[1] Global Maritime Intelligence Integration Plan, October 2005, p. 1.

[2] Ibid p. 1.